Thesis for The Degree of Licentiate of Engineering

Towards Understanding and Applying Security Assurance Cases for Automotive Systems

Mazen Mohamad

Division of Interaction Design and Software Engineering
Department of Computer Science & Engineering
Chalmers University of Technology and Gothenburg University
Gothenburg, Sweden, 2021

Towards Understanding and Applying Security Assurance Cases for Automotive Systems

Mazen Mohamad

Department of Computer Science & Engineering
Division of Interaction Design and Software Engineering
Chalmers University of Technology and Gothenburg University
Gothenburg, Sweden

This thesis has been prepared using LaTeX.
Printed by Chalmers Reproservice,
Gothenburg, Sweden 2021.

"Amateurs hack systems, professionals hack people."
- Bruce Schneier

Abstract

Security Assurance Cases (SAC) are structured bodies of arguments and evidence used to reason about security properties of a certain artefact. SAC are gaining focus in the automotive domain as the need for security assurance is growing due to software becoming a main part of vehicles. Market demands for new services and products in the domain require connectivity, and hence, raise security concerns. Regulators and standardisation bodies started recently to require a structured for security assurance of products in the automotive domain, and automotive companies started, hence, to study ways to create and maintain these cases, as well as adopting them in their current way of working.

In order to facilitate the adoption of SAC in the automotive domain, we created CASCADE, an approach for creating SAC which have integrated quality assurance and are compliant with the requirements of ISO/SAE-21434, the upcoming cybersecurity standard for automotive systems.

CASCADE was created by conducting design science research study in two iterative cycles. The design decisions of CASCADE are based on insights from a qualitative research study which includes a workshop, a survey, and one-to-one interviews, done in collaboration with our industrial partners about the needs and drivers of work in SAC in industry, and a systematic literature review in which we identified gaps between the industrial needs and the state of the art.

The evaluation of CASCADE was done with help of security experts from a large automotive OEM. It showed that CASCADE is suitable for integration in industrial product development processes. Additionally, our results show that the elements of CASCADE align well with respect to the way of working at the company, and has the potential to scale to cover the requirements and needs of the company with its large organization and complex products

Keywords:

security, assurance case, automotive, automotive systems, arguments, evidence, security claims

Acknowledgment

First of all, I would like to express my sincere gratitude to my supervisor and mentor Riccardo Scandariato for all the support, advice, patience, collaboration, and trust he provided me during this journey. I would also like to thank my co-supervisor Jan-Philipp Steghöfer for his great advice, feedback, collaboration and inspiring discussions. I also thank my examiner Ivica Crnkovic for trusting me and giving me the freedom to conduct my research.

Thank you to all my colleagues and friends at the Interaction Design and Software Engineering division for welcoming me in a very nice working environment and for all the nice social and sports activities. Special thanks to my friends whom I shared an office with: Rodi, Linda, Khaled, Joel, Mads, and Hamdi. I would also like to extend my thanks to my industrial partners at Volvo and Volvo Cars for all their support.

Finally, I wish to express my deepest gratitude to my parents, friends, and my wife Rim, who did not spare a chance to motivate me and provide me with love and encouragement. I also wish to thank my son Bassam for inspiring me every single morning.

This work is partially supported by the CASUS research project funded by VINNOVA, a Swedish funding agency.

List of Publications

Appended publications

This thesis is based on the following publications:

[A] M. Mohamad, A. Åström, Ö. Askerdal, J. Borg, R. Scandariato "Security Assurance Cases for Road Vehicles: an Industry Perspective" *International Conference on Availability,Reliability and Security ARES, 2020.*

[B] M. Mohamad, J.P. Steghöfer, R. Scandariato "Security Assurance Cases – State of the Art of an Emerging Approach" *Empirical Software Engineering Journal - To appear.*

[C] M. Mohamad, Ö. Askerdal, R. Jolak, J.P. Steghöfer, R. Scandariato "Asset-driven Security Assurance Cases with Built-in Quality Assurance" *International Workshop on Engineering and Cybersecurity of Critical Systems (ENCYCRIS), 2021.*

Other publications

The following publications were published before or during my PhD studies, or are currently in submission/under revision. However, they are not appended to this thesis, due to contents overlapping that of appended publications or contents not related to the thesis.

[a] M. Mohamad, G. Liebel, E. Knauss "LoCo CoCo: Automatically constructing coordination and communication networks from model-based systems engineering data"
Information and Software Technology Journal 92, 179-193, 2017

[b] R. Jolak, T. Rosenstatter, M. Mohamad, K. Strandberg, B. Sangchoolie, N. Nowdehi, R. Scandariato "CONSERVE: A Framework for the Selection of Techniques for Monitoring Containers Security"
In submission to The Journal of Systems & Software

[c] J.P. Steghöfer, B. Koopmann, J.S. Becker, M. Törnlund, Y. Ibrahim, M. Mohamad "Design Decisions in the Construction of Traceability Information Models for Safe Automotive Systems"
In submission to the International Requirements Engineering Conference

Research Contribution

My contribution in Paper A was mainly in the internal needs part. I, equally contributed in preparing the workshop, facilitating the brainstorming sessions and collecting the results. In the survey, I contributed the design, data collection, and analysis of results. I also equally contributed in leading the discussion in the interviews, and did the analysis of the outcome. When it comes to writing the paper, I contributed the majority of all sections, except for RQ1 results and the introduction.

In Paper B, I contributed in running the search on the three digital repositories, collecting the results, filtering the results in three rounds, conducting the snowballing search, and analyzing and screening the included studies. I also equally contributed in the sessions for identifying the assessment and inclusion/exclusion criteria. I also did the majority of the writing in all sections but the introduction and discussion, in which I contributed.

In Paper C, I contributed equally in designing the CASCADE approach. I also created the SAC based on the example use case, conducted the evaluation of the approach, and analyzed the outcome of the evaluation. In terms of paper writing, I did the majority of the writing of all sections except for the background and validation, in which I contributed equally.

Contents

Chapter 1

Introduction

Security is gaining more focus in safety-critical domains since more connectivity is needed in the services and products offered by companies in these domains. In automotive, software has become a main part of vehicles and the need for connectivity is essential to meet the market demands for functionalities and services the vehicles offer, e.g., mobile phone connectivity and navigation services. This has raised an issue when it comes to security assurance, i.e., answering the question "how do we make sure and prove that our product is secure?". This becomes an even larger issue the more complex the systems become, consisting of multiple sub-systems with many stakeholders involved, e.g., different providers for different parts.

Regulators and standardisation bodies recently started to require a structured way of security assurance for automotive products and processes. For this reason, Security Assurance Cases (SAC) were specifically required in ISO/SAE-21434 [1] to prove security conformance. Automotive companies started, hence, to study ways to create and maintain these cases, as well as adopting them in their current way of working. Assurance cases in general are not new to the automotive industry, as companies are already familiar with similar cases created for safety (safety cases), which are required by ISO-26262 [2] for functional safety for road vehicles. This opens up opportunities for knowledge transfer from the safety domain into the security domain. However, this knowledge transfer should be done cautiously and consider the differences between the two domains.

In this work, we created CASCADE, an approach for creating SAC which are compliant with the requirements of ISO/SAE-21434 and have integrated quality assurance. CASCADE is based on insights from two studies: one done in collaboration with our industrial partners about the needs and drivers of work in SAC in industry and one systematic literature review in which we identified gaps between the industrial needs and the state of the art.

As a first step, we identified and studied different factors that would drive the work with security cases in the automotive domain. We studied internal drivers, i.e., the requirements and needs from within an automotive company. We identified thirteen different scenarios in which SAC can be used. These scenarios spread over the entire life-cycle of automotive products and involve many different roles in automotive companies. These scenarios also imposed

additional requirements on SAC. E.g., the quality assurance of a SAC is essential in order for it to be useful in industry.

External drivers that impose constraints of how SAC should look like were identified by our partners at industry. This was done analyzing how SAC were referenced in different documents (regulations, standards and best practices) in the three major automotive markets (EU, US, and China). Thirteen documents where SAC was either explicitly or implicitly required, or would assist to fulfill the requirements of the documents were identified.

Based on what we learned about the internal and external needs for SAC in automotive, we conducted a systematic literature review to examine whether these needs are covered in literature or not. We systematically reviewed literature and looked for different characteristics, e.g., usage scenarios, approaches for creating SAC, and tool support. In analysing our results, we made multiple observations. Most importantly, we saw a wide variety of approaches for creating SAC, but none of them considers actual constraints and needs from the automotive domain. We also observed a lack of quality assurance of SAC in the reviewed literature. Another observation we made is the wide range of potential benefits of SAC that was reported. However, there was a gap between the internal needs identified at the automotive company, and the usages suggested in literature.

For all the reasons above, we designed our own approach for SAC creation based on what we learned from industry and literature. We focused on two main aspects:

- Align the requirements and work products of the upcoming standard ISO/SAE-21434 and the SAC (the outcome of the approach).
- Integrate quality within the cases themselves.

CASCADE, is an asset driven approach for creating security assurance cases with built-in quality assurance. We illustrated the approach using an example use case from ISO/SAE-21434 and evaluated it with help of security experts at a large automotive OEM. The evaluation showed that CASCADE is suitable for integration in industrial product development processes. The elements of CASCADE align well with respect to the way of working at the company. Additionally, CASCADE has the potential to scale to cover the requirements and needs of the company with its large organization and complex products.

1.1 Research Focus

This research work is motivated by the observation that SAC are becoming important in the safety critical domain, in particular, companies in the automotive industry.The main goal of this research is "*to support practitioners in the automotive domain to make go/no go decisions of the release of their products from a security point of view, with the help of security assurance cases*". To achieve this overall goal, we addressed the following goals in this licentiate thesis:

- **Goal 1:** to understand the specific needs concerning SAC in the automotive domain.

- **Goal 2:** to understand the state of the art about SAC in literature.
- **Goal 3:** to create and assess an approach for creating SAC taking into consideration the specific needs of the automotive domain.

To reach the goals of this thesis, we formulate the following research questions:

RQ1: What are the drivers for working with security assurance cases in the automotive domain?

This question addresses the emergence of several standards and regulations that are forcing the industry to develop a methodology for SAC in order to stay compliant and avoid legal risks. We call these the *external drivers* that will impose constraints on what SAC should look like. The need to develop a strategy for SAC is also perceived by the automotive companies as an opportunity to improve their cybersecurity development process. As such, the question also takes up the *internal drivers* related to this aspect.

RQ2: What are the gaps in the state of the art when it comes to the industrial applicability of SAC?

This question aims at identifying gaps in the state of the art with respect to the needs of companies in the automotive domain from two perspectives:

- Approaches for the creation of SAC
- Support to assist practitioner in creating SAC

RQ3: How can an approach for the construction of security assurance cases fulfill the needs of the automotive domain?

The purpose of this question is to investigate how an approach for SAC creation can be built in order to fulfill both the external and internal needs of automotive companies, as well as closing the gaps between research and the industrial needs for SAC adoption.

1.2 Context and related work

In this section, we provide a background about security assurance cases, as well as a review of related work.

1.2.1 Security Assurance Cases

Assurance cases are defined by the GSN standard [3] as "*A reasoned and compelling argument, supported by a body of evidence, that a system, service or organisation will operate as intended for a defined application in a defined environment.*"

Assurance cases can be documented in either textual or graphical forms. Figure 1.1 depicts an example of what an assurance case documented using the GSN notation looks like. The case in the example is a part of a larger case for a supermarket system.

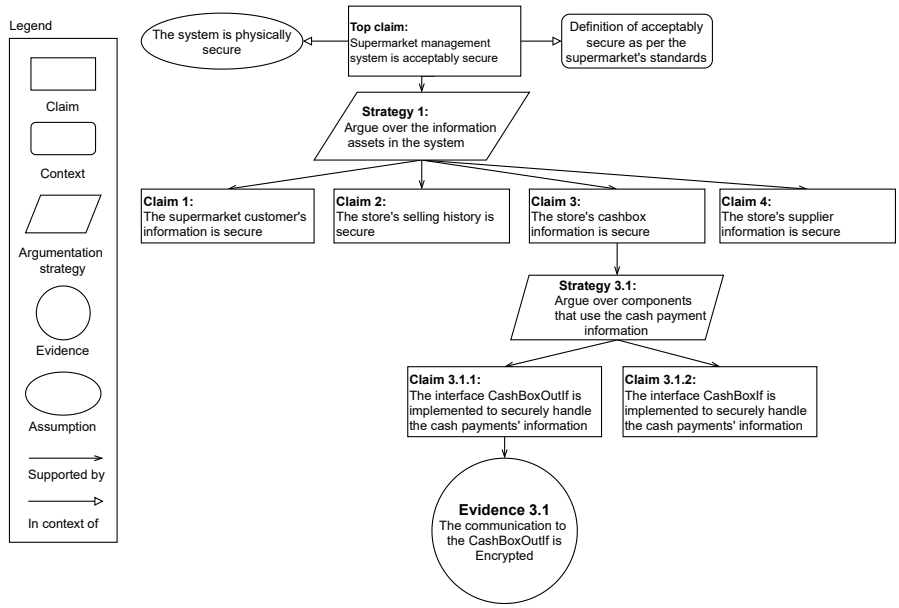

Figure 1.1: An example of a security assurance case

Assurance cases consist of two main parts: the argument and the evidence. The case in the figure consists of the following nodes: claim (also called goal), context, strategy, assumption (also called justification), and evidence (also called solution). At the top of the case, there is usually a high level claim, which is broken down to sub-claims based on certain strategies. The claims specify the goals we want to assure in the case, e.g., that a certain property is preserved. An example of a strategy is to break down a claim based on the information assets of the system as shown in *Strategy 1* in Figure 1.1. Claims are broken down iteratively they reach a point where evidence can be assigned to justify them. Examples of evidence are test results, monitoring reports, and code review reports. The assumptions made while applying the strategies, e.g., that all relevant threats have been identified, are made explicit using the assumption nodes. Finally, the scope of a claim is set using the context nodes. An example of a context is the definition of an acceptably secure system.

Assurance cases have been widely used for safety-critical systems in multiple domains [4]. An example is the automotive industry, where safety cases have been used for demonstrating compliance with the functional safety standard ISO 26262 [2, 5, 6]. Another example is the medical domain, where safety cases where used to assure the safety of medical devices [7]. However, there is an increasing interest in using these cases for security as well. For instance, the upcoming automotive standard ISO 21434 [1] explicitly requires the creation of cyber-security arguments. SAC are a special type of assurance cases where the claims are about the security of the system in question, and the body of evidence justifies the security claims.

1.2.2 Related work

In this section, we present the related work to the main contribution of this thesis, CASCADE. It is an asset-driven approach for creating SAC with built-in quality assurance, inspired by ISO/SAE-21434 standard for cybersecurity in automotive. Hence, we introduce the main papers which use assets as argumentation strategies, are based on security standards, or are conducted in the automotive domain.

1.2.2.1 Asset-based approaches

Assets are artefacts of value to a certain organization, project, or system. Researchers have been exploring several asset-based approaches for creating the argument part of SAC. These approaches use assets and their decomposition as strategies to break down claims in SAC.

Biao et al. [8] suggest dividing the argument into different layers, and using different patterns (one per layer) to create the part of the argument that corresponds to each layer. Assets are considered as one of these layers, and the pattern used to create it includes claims that the assets are "under protection", and strategies to break down critical assets. In contrast to our work, Biao et al. [8], however, do not consider the quality of the cases and only focus on creating arguments without touching upon the evidence part.

Luburic et al. [9] also present an asset-based approach for security assurance. The info used in their approach is taken from: *(i)* asset inventories; *(ii)* Data Flow Diagrams (DFD) of particular assets and the components that manipulate them; and *(iii)* the security policy that defines protective mechanisms for the components from the previous point. They propose a domain model where assets are the center pieces. The assets are linked to security goals. The argument considers the protection of the assets throughout their life-cycles by arguing about protecting the components that store, process, and transmit those assets. The SAC they provide is very high level and includes two strategies: "reasonable protection for all sensitive assets" and arguing over the data-flow of each related component. The authors illustrate the approach with a conference management system example. They state that the main limitations of their are asset and data flow granularity. In our work, we also consider the assets to be the driver of our approach, but we extend the argument to reach the level of concrete security requirements. We also derive our strategies from an industrial standard and validate our approach in collaboration with an OEM. Furthermore, we extend our approach to include case quality aspects.

1.2.2.2 Standard-based approaches

Using standards to extract requirements for creating the arguments of SAC has been done in multiple studies. However, none of these studies targets the upcoming standard ISO/SAE-21434 for cybersecurity in automotive. Finnegan et al [10, 11] present a security case framework for the area of medical device security assurance. Their framework incorporates multiple standards and best practice documents as a guidance to develop a security argument pattern. The pattern provides a "comprehensive matrix showing the link between the security

risks, associated causes, the mitigating security controls and evidence of those controls being implemented to establish the security capability."

Ankrum et al. [12] studied how requirements from standards in safety-critical domains can be mapped to assurance cases using the most common notations for documenting assurance cases Goal Structuring Notation (GSN) and ASCAD (Claims – Arguments – Evidence). One of the standards used in the study was the Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408:1999 [13], and the researchers describe challenges they encountered while conducting the mapping and lessons learned.

In our work, we have used the upcoming ISO/SAE 21434 standard to structure an approach for creating SAC, but also considered the industrial needs from the automotive domain.

1.2.2.3 Studies in automotive

Few studies about SAC have been conducted or evaluated in the automotive domain. Cheah et al. [14] in their study "Building an automotive security assurance case using systematic security evaluation" review security engineering in the automotive industry, and the challenges to introducing a security engineering process in this domain, e.g., the overhead required to establish a security mechanism in general, and the diversity of the vehicles with many Parameters and configurations. The authors presents a classification approach of security test results using security severity ratings. This classification can be included in the security evaluation, which may according to the study be used to improve the selection of future test cases, as well as evidence when creating security assurance cases. The paper includes two case studies that demonstrate the method. The first case was done with a Bluetooth connection to the infotainment system of a vehicle, and the second was done on an aftermarket diagnostics tool. The results of both studies are severity rated evidences which could be used to prioritize countermeasure development, and to add evidence to security assurance cases. No security assurance case is actually created, but rather severity rated evidences which the authors claim can be used in a security assurance case.

1.3 Methodology

This section summarizes the research methodology applied to answer the research questions of this thesis. RQ1 was answered through qualitative research methods. RQ2 was addressed using a systematic literature review and RQ3 was answered using the Design Science Research methodology.

1.3.1 Qualitative research methods

We used various qualitative research methods in Paper A to answer the first research question *"What are the drivers for working with security assurance cases in the automotive domain?"*, as shown in Figure 1.2. These include a workshop, a survey, and one-to-one interviews. In Figure 1.2, The part marked

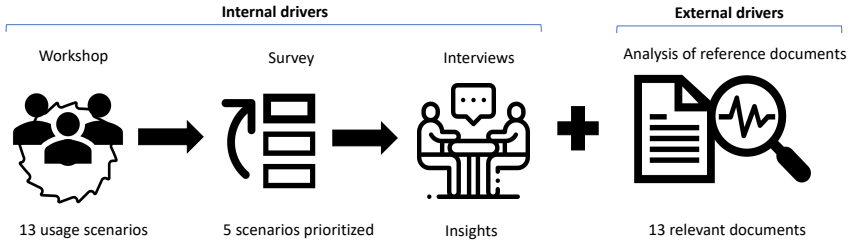

Figure 1.2: Qualitative research methods – Paper A

as *internal needs* was contributed by the author of this thesis, while the external needs part was contributed by co-authors of Paper A.

1.3.1.1 Workshop

We conducted a workshop at a large automotive OEM to elicit usage scenarios related to SAC. We invited stakeholders from different backgrounds and different parts of the organization. We had 12 participants and three moderators contributing. We divided the participants into three groups of 4, making sure to spread similar roles and competences among the groups. E.g., we had three participant who were familiar with safety cases, so we assigned them to different groups. We asked the groups to brainstorm for 45 minutes on usage scenarios for security assurance cases, and to describe them as user stories, like "As a «role» I would use security assurance cases for «usage»" [15]. Each user story corresponds to one usage scenario. We explicitly asked the participants to come up with real-life scenarios in the context of their company. The participants shared their usage scenarios on a whiteboard, and we compiled a set of distinct scenarios as an outcome of this step and an input to the next step.

1.3.1.2 Prioritization and interviews

At this step, we wanted to dig deeper and get a better understanding of the most important scenarios. We also wanted to acquire the point of view of more diverse stakeholders. Hence we had to prioritize the usage scenarios and identify stakeholders to be interviewed for the top ones.

Concerning the prioritization, we aimed at getting expert opinions on which usage scenarios are of most value to the company, from a security perspective. We sent out the scenarios collected from the workshop to 10 security experts from an automotive OEM, and asked them to select the top five scenarios by assigning a rank from 1 to 5 to them, where 5 is assigned to the most valuable scenario for the company.

Afterwards, we selected the top five usage scenarios and identified a key stakeholder for each. Finally, we conducted in-person interviews with these stakeholders to gain a deeper understanding of the usage scenarios. The interviewees were selected based on the relevance of their expertise to the actors

of the user stories in the corresponding usage scenarios. For example, the actor of one of our top usage scenarios is a *legal risk owner*. Hence, we selected an interviewee who has extensive experience in law and has the role *senior legal counsel* in the company.

We organized each interview into four parts, according to the following themes:

i **Value** In the first part, we focus on the value that SAC might bring to the stakeholder in terms of, e.g., efficiency, and quality management. The objective of the discussion is to picture the 'status quo' (e.g., to understand how the level of security is currently appraised) and the expectations (i.e., how things should improve).

ii **Content and structure** The focus of this part is to get the interviewees' technical opinions on how the content and structure of SAC should be, e.g., in terms of level of detail and types of claims.

iii **Integration** This part is about understanding how SAC could be integrated with the current way of working, and whether it could fit in the current activities, or would require modifications to the process.

iv **Challenges and opportunities** The last part of the interview is about understanding the challenges and opportunities that the stakeholders foresee in applying SAC.

In each interview, there was an interviewer, an interviewee, and a security expert who acted as a discussion enabler. We recorded the interviews, and used the recordings to extract a transcript for each interview. To analyze the data, we used deductive coding using codes corresponding to our predefined themes. The analyzed data was then sent to the corresponding interviewees for validation and additional comments.

1.3.1.3 Analysis of documents

To gain an understanding of the external drivers of SAC work, a knowledge base of documents relevant to cybersecurity, which was created and maintained by an industrial partner was used. This knowledge base consist of standards, regulations, guidelines, best practices, etc applicable for various markets, and includes, among other things, information regarding the categorization of requirements, their relevance, the parts of the organization that is affected, and which life-cycle phases of the products are impacted. Co-authors of Paper A analyzed the documents for explicit references to security assurance cases or their parts. They also looked for implicit relationships to SAC, e.g., when the documents include requirements of processes for identification, assessment and mitigation of vulnerabilities. An SAC can then be used to show how this requirement is fulfilled listing the demanded processes and the evidence for them.

1.3.2 Systematic Literature Review(SLR)

Systematic Literature Reviews (SLR) are conducted to collect and analyze data related to a specific research question [16]. We conducted an SLR in

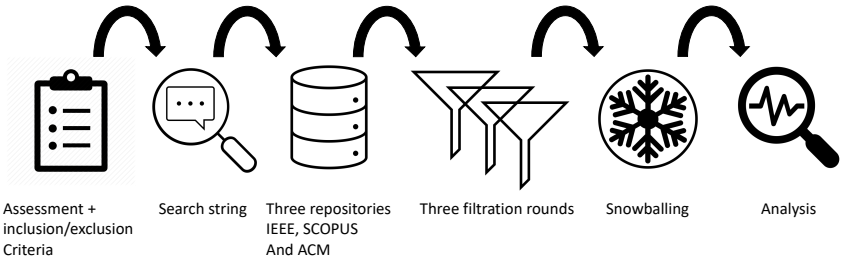

Figure 1.3: Systematic Literature Review steps – Paper B

Paper B to gain an understanding of existing work in security assurance. In particular, we looked for approaches for creating security assurance cases and evidence concerning their validity, support to facilitate the adoption of SAC, and rationale to support the adoption of SAC. We followed the guidelines introduced by Kitchenham et al. [16], and conducted the study in six steps as depicted in Figure 1.3.

In the first step, we carefully constructed the assessment criteria for each of our research questions and the inclusion/exclusion criteria for the retrieved papers. This was done in a series of brainstorming sessions including the three authors of the study.

The second step was creating the search string. In order to maximize the chance of obtaining all relevant papers in the field we familiarized ourselves with the specific terminology used by researchers in the field of security assurance. This was done by conducting a manual search for papers related to security assurance cases that were published in the past five years in multiple venues with high visibility in the security domain. We executed the query on three libraries (IEEE Xplore, ACM Digital Library,and Scopus) and got a total of 8440 results.

In the next step, we applied the inclusion/exclusion criteria on the results in three filtration rounds. In the first one, we filtered based on the title and keywords, which reduced the number of included studies to 211. In the second filtering round, we applied the inclusion and exclusion criteria to the abstracts and conclusions of the 211 remaining studies. After this step, the number of studies was reduced to 49. In the last filtering round, we fully read the remaining 49 papers, applied the inclusion and exclusion criteria on the whole text, and ended up with 44 included studies. We also looked at the references in the included papers and performed *backward snowballing* [17]. In this step, we did not restrict the search to only peer-reviewed studies in order to allow for potential gray literature to be included. This resulted in including additional 7 papers (including 2 technical reports) in our review.

Finally, we analyzed the 51 included studies based on our defined assessment criteria to answer our research questions.

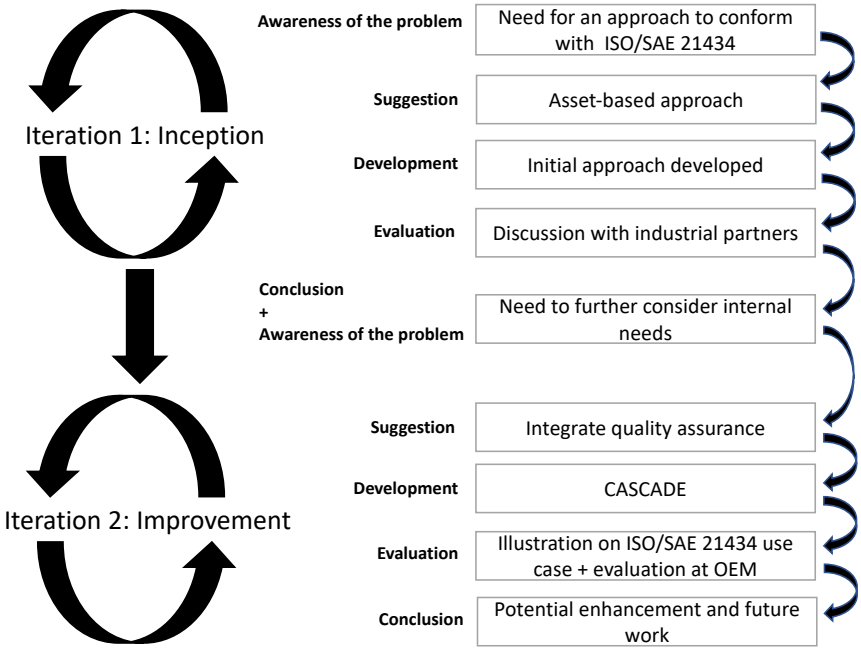

Figure 1.4: Two-iteration Design Science Research – Paper C

1.3.3 Design Science Research (DSR)

Design science research is a problem-solving methodology, which aims at developing artefacts to extend existing boundaries in a given context [18]. In paper C, we conducted two research iterations, following the design science guidelines proposed by Hevner et al. [18] and the five-step process proposed by Vaishnavi and Kuechler [19], which consists of the *awareness of the problem*, *suggestion*, *development*, *evaluation* and *conclusion* steps. The two-iteration process is depicted in Figure 1.4.

The first iteration, *initiation*, aimed at addressing the needs for security assurance cases which were identified in Paper A. Specifically, we aimed at investigating an asset-based approach for the creation of security assurance cases, in order to assist automotive companies to fulfill their needs to conform with the upcoming ISO/SAE-21434 standard. We suggested an initial asset-based approach and used an online case for a supermarket system [20] to illustrate the outcome of the approach. The approach and the outcome of the illustration were discussed with security experts at two large automotive OEMs. The main input from the companies was focused on the need to align the structure of the approach with the internal way of working at the companies, which is also one of the internal needs identified in Paper A. Another aspect of improvement that emerged from the evaluation of the initiation iteration is the need for a mechanism to assure the quality of the approach's outcome.

In the second iteration *improvement*, we aimed at improving the artefact

(asset-based approach) by incorporating the experience gathered in the first iteration. We created CASCADE, an asset-based approach for SAC creation with built-in quality assurance. The structure of CASCADE is inspired by the requirements and work products of ISO/SAE-21434, and takes into consideration the need to quality assure the outcome, as well as the way of working at the automotive companies we consulted in the first iteration. To evaluate CASCADE, we applied it on an example case of a headlamp item from ISO/SAE-21434, and presented the outcome to security experts at an OEM. As a conclusion, we identified areas for future enhancement of CASCADE to fulfill a wider range of the internal needs of the company.

1.4 Contributions

In this section, we provide a summary of the main contributions of each paper towards answering our research questions.

1.4.1 RQ1: What are the drivers for working with security assurance cases in the automotive domain?

To answer this research question we conducted the study presented in Paper A. We investigated the internal drivers of SAC work in automotive and contextualized the results based on the external drivers which were identified by our co-authors, as explained in Section 1.3.1.3

Our results clearly indicate potential value of using SAC at the company. They show that SAC can be used by a variety of *stakeholders*, e.g., product owners and compliance team members, for a variety of *purposes*, e.g., quality assessment and communication with suppliers, in all the *phases of an automotive product's life-cycle*, e.g., design and development.

1.4.1.1 Internal drivers of SAC in the automotive industry

What drives the SAC work in an automotive company is the value the cases can bring to people in different roles in the company. Hence, we identified 13 usage scenarios for SAC in an automotive company. We also prioritized these usage scenarios based on the potential added value to the company, and identified the top 5 scenarios, which are shown in Table 1.1

To gain a better understanding of the usage scenarios, we conducted interviews with corresponding roles and as a result, we extracted a set of drivers for companies wanting to adopt SAC in their work, as shown in Table 1.2.

1.4.2 RQ2: What are the gaps in the state of the art when it comes to the industrial applicability of SAC?

To answer this question, we need to know what the industrial needs are, which is covered in Paper A. Additionally, we need to know what exist in literature, and accordingly, we can identify the gaps. Paper B contributes with a Systematic Literature Review in which multiple research questions regarding the applicability of SAC in industry are studied. Specifically, we

Table 1.1: Top 5 usage scenarios identified at an automotive company

US 2	As a member of the compliance team, I would use detailed SAC to prove to authorities that the company has complied to a certain standard, legislation, etc., and show them evidence of my claim of compliance.
US 6	As a product owner, I would use SAC to make an assessment of the quality of my product from a security perspective, and make a road-map for future security development.
US 12	As a legal risk owner, I would use SAC in court if a legal case is raised against the company for security related issues. I would use the SAC to prove that sufficient preventive actions were taken.
US 8	As a member of the purchase team, I would include SAC as a part of the contracts made with suppliers, in order to have evidence of the fulfillment of security requirements at delivery time, and to track progress during development time.
US 3	As a project manager, I would use SAC to make sure that a project is ready from a security point of view to be closed and shipped to production.

studied the motivations for creating and using SAC as reported in literature. We also studied different reported approaches for SAC creation, as well as their validations. Lastly, we studied the reported support for SAC creation as reported in literature.

1.4.2.1 Wide variety of approaches, but not enough to cover industrial needs

The literature includes a rich variety of studies which explore approaches for creating SAC, especially when it comes to the argumentation part. However, theses approaches do not consider the specific needs of companies in a specific industry, e.g., automotive.

The variety in approaches gives organizations the possibility to choose those that fit their way of working and the security artefacts they produce. For example, a company that works according to an agile methodology could choose to adopt an SAC approach for iterative development [21]. However, this choice has to consider constraints of the applicability of the approach, including benefits and challenges of its adoption, e.g., the impact on the the way of working. These aspects are not discussed in the literature and the burden is left to the adopter.

Another example is the question of conformance with different standards. While this has been discussed in literature, there is a lack of studies which systematically assess different approaches based on their ability to help achieving conformance with a certain standard. To generalize this, we observed that there is a lack of studies which compare different approaches in different contexts. In consequence, from an industrial perspective, organizations need to select

Table 1.2: Drivers of SAC work in automotive companies

Driver	Description
The importance to cover both product and process to comply with regulations and standards	Several of the security-related standards/regulations contain both requirements on processes and the product. The processes include how to develop the product in a secure manner as well as keeping the product secure after its release.
The need for SAC on whole products over sub-projects	In industries producing complex products, e.g., automotive, it is common that the products are organized in multiple projects. Additionally, the changes to these products are also done using projects (commonly called delta projects). In this case, SAC should be created on a product level rather than a project level.
Essential that SAC work follows the development process	It is possible to build SAC for existing products, but going forward, it is important to embed the work on SAC into the development process at the organization
The need to actively assess the quality of SAC	SAC are going to serve multiple purposes within the organization with different levels of criticality. Therefore, it must be clear what the quality level of each SAC is, so that they are not used in the wrong context.
A common language is key to smooth collaboration with suppliers	When it comes to working with suppliers, the SAC should be built using an exchangeable format. This is to enable the SAC created by the suppliers to be integrated with the SAC of the corresponding product.
The importance to plan for shared ownership with suppliers	The suppliers might require to keep parts of the SAC private (e.g., some evidence). In this case, it is important to have a mechanism to keep ensuring the overall quality of the SAC, e.g., by introducing a black-box with meta-information. Additionally, the ownership of the whole case has to be considered, as the complete SAC would not be in the hands of a single stakeholder.
The challenging nature of working with SAC	Working with SAC is not trivial and comes with many challenges. Traceability and change analysis were considered main challenges by the majority of the participants. Additionally, finding the right competences to carry out the SAC-related work, role identification and description, and acquiring the right tools and integrating them in the organizations tool chain were also considered major challenges.

suitable approaches in an exploratory way, which can be highly time and resource consuming.

The studies presenting new approaches also lack the discussion of the granularity level that is possible or required to achieve using each approach. We believe that future studies should take into consideration the possible usages for SAC created using different approaches, and discuss the required granularity level based on that. For example, would an SAC created through the security assurance-driven software development approach [22] be useful to companies which outsource parts of their development work to providers? In that case, on which level should these cases be created, e.g., on the feature level or on the level of the complete product?

1.4.2.2 Lack of quality assurance

Quality assurance is the weaker part of the literature reviewed in Paper B. We talk here about three main things. First is the quality of the outcomes when it comes to their applicability in practice. We have seen scarcity of industrial involvement. The reason might be a lack of interest, which contradict the reported motivations and usage scenarios, or simply because it is hard to get relevant data from industrial companies to validate the outcomes, as security-related data is considered to be sensitive (as we mentioned earlier). Furthermore, with the exception of a few cases, the creation and validation of SAC in literature is done by the authors of the studies. We believe that this contributes heavily to the lack of information addressing challenges and drawbacks of applying SAC in a practical context.

The second issue is the generalizability of the approaches with regards to the used argumentation strategies. The approaches we reviewed use a wide variety of argumentation strategies, e.g., based on threat analysis, requirements, or risk analysis. However, they lack validations and critical discussions as to whether the approaches work only with the used strategies or can use other strategies as well. We suggest to validate these approaches based on different types of strategies in future research.

The last point is the lack of mechanisms for including quality assurance within the SAC. We learned in RQ1 that it is essential for the argumentation provided in SAC to be complete in order for them to be useful. For that there needs to be a mechanism to actively assess the quality of the arguments to gain confidence in them. This is not addressed in literature apart from a few studies where it has been partially addressed, e.g., [23–25]. Similarly, the evidence part also needs to be assessed. e.g., by introducing metrics to assess the extension to which a certain evidence justifies the claim it is assigned to. The inter-relation between claims and evidence needs to be addressed to assess whether a claim is fully justified by the assigned evidence or not.

1.4.2.3 Imbalance in coverage

Multiple needs and drivers, e.g., managing working with suppliers, quality assurance of SAC, and organization-related issues are not covered in literature. This indicates a weakness in the approaches, as elements of SAC cannot be

evaluated in silos. For example, if we take an approach to create security arguments, how would we know which evidence to associate with these? Moreover, we will not be able to assess whether we actually reach an acceptable level of granularity for the claims to be justified by evidence. The same thing applies to the evidence part. If we only look at the evidence we will not be able to know which claims the suggested evidence can help justify. To be able to evaluate the evidence, they have to be put in context with the rest of the SAC. When reviewing the studies that focus on one element of SAC, we were not able to find any links to related studies focusing on the remaining elements, which indicates incompleteness of the approaches.

When it comes to other areas, the assessment and quality assurance of SAC is rarely covered, as we discussed in the previous sub-section. Furthermore, there is a lack of studies covering what comes after the creation of SAC. In particular, for SAC to be useful, they have to be updated and maintained throughout the life-cycles of the products and systems they target. Otherwise, they become obsolete, according to what we learned in Paper A. Particularly, there need to be traceability links between the created SAC and the artefacts of these products and systems. Many SAC approaches use GSN, which allows to reference external artefacts using the context and assumption nodes. However, these nodes are rarely exploited in the examples provided in the studies we reviewed. Moreover, there is a lack of studies targeting the organizational aspects of working with SAC, e.g., the ownership of SAC and how to handle sub-cases when working with suppliers.

1.4.3 RQ3: How can an approach for the construction of security assurance cases fulfill the needs of the automotive domain?

The three papers included in this thesis contribute towards answering RQ3. We built on the gained knowledge when answering RQ1 and RQ2 to create an approach for SAC creation. The approach CASCADE is the main contribution of Paper C. It is an asset-driven approach with built-in quality assurance.

1.4.3.1 Design goals of CASCADE

CASCADE is inspired by the upcoming standard for cybersecurity in automotive SAE/ISO-21434 [1]. Conformance with this standard has been identified as one of the most important drivers for SAC work in Paper A, and it has not been covered in any of the papers included in the SLR of Paper B. CASCADE was designed to achieve the following goals:

- Make assets the driving force of the SAC to allow creating security assurance based on what is valuable in the system.
- Embed quality assurance in the approach to make sure the outcome satisfies the desired quality by the adopting entity.
- Divide the approach into different layers and blocks, so that different people can work on them in different development phases.

- Enable re-usability and scalability to prevent overhead and work repetition while creating SAC on lower-level items.

1.4.3.2 Structure of the approach

CASCADE consists of blocks which correspond to the requirements and work products of SAE/ISO-21434. Figure 1.5 shows these blocks.

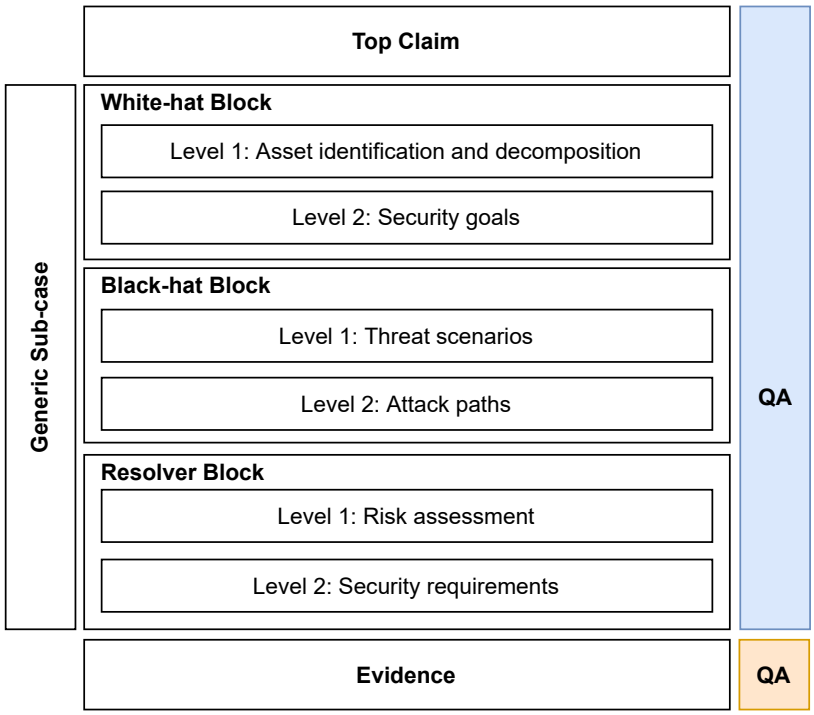

Figure 1.5: The CASCADE approach for creating security assurance cases

Top Claim consists of the top security claim of the artefact in question. It also includes the context of the claim and assumptions made to set the scope of the claim.

Generic sub-case helps achieve the goal of preserving re-usability and scalability. It contains a sub-case that is applicable not only to the artefact for which the SAC is being created, but instead to a larger context. For example, if a company defines a cybersecurity policy, enforced by cybersecurity rules and processes, then the policy can be used in security claims for all its products.

White-hat This block starts with the identification of assets, which is the driver of our approach, as per our design goals. Asset identification is done by conducting an analysis to find the artefacts of the system that are likely

to be subject to an attack. To link the assets to the main claim, we identify which assets exist and which components use or have access to these assets. To decompose assets, we look into the types of the identified assets. This gives an indication whether the asset would have implications on the local part of the vehicle (one electronic control unit/ECU), or on a bigger part of the vehicle (multiple ECUs).

We also look into the relations among assets, e.g., dependability. To link the asset to the lower level in the approach, i.e., the security goals, we identify the relevant security properties for the assets. Specifically, we look into the Confidentiality, Integrity, and Availability (CIA) triad. When we have identified the relevant security properties for each asset, we create claims representing the security goals[1].

Black-hat In this block, we aim to identify the scenarios that might lead to not fulfilling the identified security goals and hence cause harm to our identified assets. When we have identified the claims about the achievement of security goals, we proceed by identifying the threat scenarios and creating claims for negating the possibility of these scenarios. We connect these claims to the corresponding claims about achieving security goals. We then identify possible attack paths which can lead to the realization of a threat scenario. Each threat scenario might be associated with multiple attack paths. We then claim the opposite of these attack paths.

Resolver This block is the last one in the argumentation part of the CASCADE approach. It links the claims derived from the attack paths to the evidence. In this level, we assess the risk of the identified attack paths. Based on the risk level, the creators of the SAC create claims to treat the risk by, e.g., accepting, mitigating, or transferring it.

Requirements At this point, requirements of risk treatments identified in the previous level are to be expressed as claims. This level may contain multiple decomposition of claims, based on the level of detail the creators of the SAC wish to achieve, which is driven by the potential usage of the SAC. For instance, if the SAC is to be used by a development team to assess the security level, this might require a fine grained requirement decomposition which might go all the way to the code level. In contrast, if the SAC is to be used to communicate security issues with outside parties, a higher level of granularity might be chosen. In either case, it is important to reach an *"actionable"* level, meaning that the claims should reach a point where evidence can be assigned to justify them.

Evidence The evidence is a crucial part of an SAC. The quality of the argument does not matter if it cannot be justified by evidence. In our approach, evidence can be provided at any block of the argumentation. For example, if it can be proven in the black-hat block that a certain asset is not subject to any threat scenario, then evidence can be provided and the corresponding

[1] A security goal is preserving a security concern (CIA) for an asset [26]

claims can be considered as justified. If the creators of the SAC cannot assign evidence to claims, this is an indication that either the argument did not reach an actionable point or that there is a need to go back and make development changes to satisfy the claims. For example, if we reach a claim which is not covered by any test report, then there might be a need to create test cases to cover that claim.

Case Quality Assurance assists the achievement of our design goal to embed quality assurance in CASCADE. We consider two main aspects of quality assurance for SAC. The first aspect is *completeness* which refers to the level of coverage of the claims in each argumentation level of the SAC. Each level in CASCADE includes at least one strategy. For each strategy, we add at least one completeness claim that refines it. The role of this claim is to make sure that the strategy covers all and only the relevant claims on the argumentation level. The completeness also relates to the context of the argumentation strategy. The context provides the information needed to determine if the completeness claim is fulfilled or not.

The second aspect is *confidence* which indicates the level of certainty that a claim is fulfilled based on the provided evidence. This is used in each level of a security assurance case where at least one claim is justified by evidence. The confidence aspect is expressed as a claim, which takes the form: "The evidence provided for claim X achieves an acceptable level of confidence". What makes an acceptable level of confidence is defined in the context of the strategy. The confidence claim itself must be justified by evidence.

1.4.3.3 Evaluation of CASCADE

In order to evaluate CASCADE, we collaborated with a security expert from the cybersecurity team at Volvo Trucks, which is a leading OEM that manufactures trucks in Sweden. We conducted several sessions during the development of CASCADE where we discussed the approach, its limitations and possible enhancements. When the approach was fully developed, we conducted a final evaluation session with the expert. We used the headlamp example from ISO/SAE-21434 as a context for this discussion. We then presented our approach and the example case for the headlamp item. The expert evaluated the approach by discussing what the overall structure of an SAC should look like from the company's perspective in order to satisfy the requirement for security cases in ISO/SAE-21434 and mapping the different elements of the example case to the internal way of working. The expert also provided insights on how to further enhance the approach.

Figure 1.6 shows the different security activities at the company along with the corresponding CASCADE block. A link between an activity and a block indicates that the outcomes of the activity are used to create the SAC elements in the corresponding block. As shown in the figure, CASCADE aligns well with the way of working at the company.

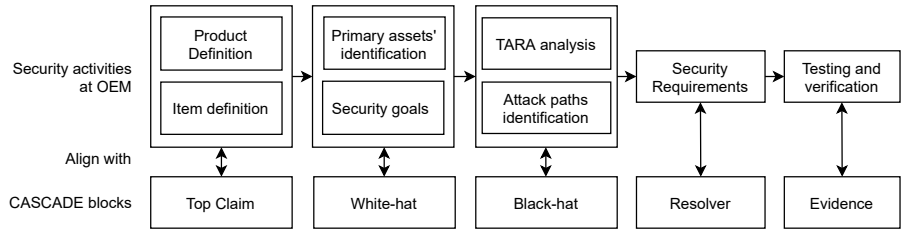

Figure 1.6: Mapping of the company's security activities to CASCADE blocks

1.5 Threats to validity

In this thesis, we consider the internal and external categories of validity threats as defined in [27], and described in [16, 28].

In terms of *external validity*, we are aware that the general validity of our results in Paper A and Paper C could be limited to the companies involved in the study. Also, the companies are from the same country. Therefore, the results might not directly translate to companies with a different culture. However, the involved companies are of high profile, quite large and compete at the international level. Therefore, they are able to provide a quite broad perspective on the entire automotive industry. In any case, the results presented in this paper are an important first important step towards a larger survey study involving more companies and professionals, internationally.

In terms of *internal validity* we consider several aspects. In the the prioritization of the usage scenarios in Paper A, there is a risk that the selection of the top scenarios was biased by present market pressure towards compliance to the upcoming standards. Another limitation is the selection of the participants of the workshop and interviews of Paper A as well as the evaluation of Paper C, as it was based on expertise and availability (convenience sampling). However, In Paper A, we have a balance mix of participants with different types of expertise: security, product development, business, and legal, and in Paper C we have an experienced security expert. This provides us with enough confidence that the results are representative of the expectations and needs across the studied companies.

The work of conducting the SLR in Paper B was done by one researcher. This means that applying the inclusion / exclusion criteria in each of the four filtering rounds was done by one person. This imposes a risk of subjectivity, as well as a risk of missing results, which might have affected the internal validity of this study. To mitigate this, a preliminary list of known good papers was manually created and used for a sanity check of the selected and included papers. Additionally, a quality control was performed periodically by the other authors to check the included and excluded studies.

Another threat to validity in the SLR is publication bias [16]. This is due to the fact that studies with positive results are more likely to get published than those with negative results. This could compromise the conclusion validity of the SLR, as in our case we did not find any study that is, e.g., against using SAC, or which reported a failed validation of its outcome. In Paper B, we have

partially mitigated this threat by also including a few technical reports (i.e., non peer-reviewed material). These papers have been identified as part of the snowballing, as we didn't restrict to peer-reviewed papers.

When it comes to the reliability of the SLR, we believe that any researcher with access to the used libraries will be able to reproduce the study, and get similar results plus additional results for the studies which get published after the work of the SLR is done.

In Paper C, we used an example from ISO/SAE-21434 to illustrate CASCADE. However, there is a risk that the example does not represent actual cases from industry. We believe that the structure of the example case is what is important for the evaluation rather than the actual content, as discussed and confirmed by the security expert who ran the evaluation at the OEM.

1.6 Conclusion

In this work, we have created CASCADE, an asset-driven approach for the creation of security assurance cases with built in quality assurance. CASCADE was inspired by the structure of the upcoming ISO/SAE-21434 standard for cybersecurity in automotive. We have identified the drivers of security assurance case work in the automotive industry by investigating and analyzing requirements and usage scenarios for these cases in the industry. We have also systematically reviewed literature of SAC and identified gaps between what is available in literature and what the industry needs. We utilized what we learned from the industry and the gaps we found in literature to design CASCADE. We evaluated this approach with a security expert at a large automotive OEM. An example case available in ISO/SAE-21434 was used to illustrate the approach, and the evaluation showed that the cyber-security activities at the company aligns well with the structure of CASCADE.

1.7 Future work

In this section, we discuss the future work, which will build on the findings of this thesis to achieve the overall goal of my PhD thesis, as discussed in Section 1.1.

Further development of CASCADE CASCADE has been designed to close gaps between literature and industrial needs when it comes to adopting SAC. We will continue to develop CASCADE to further close these gaps. In particular, we the future development will target:

- The maintenance of SAC, i.e., how to enable updating the cases following changes that are made to the system in question or to the artefacts used to build the case using traceability links.

- Organizational matters, i.e., how the work in SAC would affect the day to day work in an automotive company, and what impact it would have on the enterprise architecture of these companies.

- Work on the evidence part of SAC. In particular, we want to study the available evidence in automotive companies and assess what support is needed to continuously updated them in the SAC.
- CASCADE was inspired by the structure and requirements and work products of SAE/ISO-21434. However, there are other regulations and standards which require SAC, as we have seen in Paper A. We plan to study these requirements and reflect them in the structure of CASCADE.

Evaluation of CASCADE To assess CASCADE, we plan to evaluate it by including a larger community of automotive companies and security experts. The plan to base the evaluation on the eventual added value of CASCADE to the company. Additionally, we plan to study the application of CASCADE in other safety-critical domains, e.g., the medical domain, which includes different organizational structures to the automotive companies which we have been targeting. Moreover, we plan to reach out to stakeholders in the software engineering domain, e.g., architects with a questionnaire to evaluate CASCADE. This is mainly to eliminate the potential bias to the companies we collaborate with.